

# **EXHIBIT 56**

Curling, Donna v. Raffensperger, Brad

Page 1

THE UNITED STATES DISTRICT COURT  
FOR THE NORTHERN DISTRICT OF GEORGIA  
ATLANTA DIVISION

DONNA CURLING, et al.,  
Plaintiffs,

CIVIL ACTION FILE

vs.

NO. 1:17-CV2989-AT

BRAD RAFFENSPERGER, et  
al.,

Defendants.

-----

VIDEOTAPED DEPOSITION OF  
ANDREW W. APPEL, Ph.D.  
TAKEN BY REMOTE VIDEOCONFERENCE

January 27, 2022

7:33 a.m.

REPORTED REMOTELY BY:  
LAURA R. SINGLE, CCR-B-1343

1 Q. And if you'll bear with me here, 4.11 there  
2 that you quote in your declaration, it reads:  
3 Elections should be conducted with human readable  
4 ballots. These may be marked by hand or by machine  
5 using a ballot marking device. They may be counted  
6 by hand or by machine using an optical scanner.

7 Is that correct?

8 A. That's what it says.

9 Q. In paragraph 34 there you state: Our report  
10 represents the true scientific consensus not only of  
11 the committee itself but also to the best of our  
12 ability of the broader scientific community.

13 Do you see that?

14 A. I see that.

15 Q. Okay. And at the time you wrote this  
16 declaration, you believed that to be accurate?

17 A. The scientific consensus at the time I wrote  
18 that declaration was in flux. It certainly  
19 represents the true scientific consensus as of June  
20 of 2018 when that National Academies report was  
21 written. Since June of 2018, you know, new science  
22 developed.

23 Q. I'm going ask you that question again.

24 At the time you wrote this declaration, was  
25 that your opinion that's contained there in paragraph

1 declaration you're responding to the November 2019  
2 declaration of Dr. Gilbert; but in the course of my  
3 questions, if you have any reason to doubt me on  
4 that, just let me know if you want to take some time  
5 to look at it a little further. Okay?

6 A. All right.

7 Q. So if you'll turn with me here to page 6,  
8 paragraph 21.

9 A. All right.

10 Q. And you see the references to BMDs here,  
11 right?

12 A. Yes.

13 Q. So if I told you that at this time Georgia  
14 was transitioning to the BMD system, do you have any  
15 reason to doubt me on that?

16 A. No.

17 Q. And you say there in the last sentence of  
18 paragraph 21: The outcomes of elections conducted on  
19 current BMDs, therefore, cannot be confirmed by  
20 audits.

21 Do you see that?

22 A. Yes.

23 Q. And you're quoting out of your paper there,  
24 right?

25 A. Yes.

1 Q. And you still believe that to be the case?

2 A. Yes.

3 Q. If you'll flip a couple of pages over here  
4 to paragraph 20 -- I'm sorry. Yes, paragraph 28,  
5 page 8.

6 A. Got it.

7 Q. Do you see there where you say in paragraph  
8 39A: Professor Gilbert opines that hand-marked paper  
9 ballots cannot be audited because some voters might  
10 make imperfect marks?

11 Do you see that?

12 A. Yes.

13 Q. Okay. I'm going to mark another exhibit for  
14 you here and these two, the one you're looking at now  
15 and this next one, we will flip back and forth a  
16 decent bit on.

17 (Exhibit 6 was marked for  
18 identification, attached at the end of  
19 the original transcript.)

20 BY MR. MILLER:

21 Q. If you'll just let me know when you see that  
22 on your end.

23 A. What number would this exhibit be?

24 Q. This is going to be Exhibit Number 6.

25 A. Okay. I've got it.

1 accurately have written Professor Gilbert opines  
2 that hand-marked paper ballots would lead to a  
3 worst case scenario for audits.

4 BY MR. MILLER:

5 Q. So if you go back to Exhibit 5.

6 A. All right.

7 Q. Paragraph 30 is the next page over from  
8 where we just were.

9 A. Yes.

10 Q. And you say: He writes ambiguous marks  
11 cannot occur on a BMD. The voter's intent is clear  
12 on the ballot summary.

13 Do you see that?

14 A. Yes.

15 Q. Do you believe ambiguous marks can occur on  
16 a BMD?

17 A. I believe that ambiguous marks are highly  
18 unlikely to occur on a BMD, but that's not at all the  
19 same as what the second part of Dr. Gilbert's  
20 sentence says that the voter's intent is clear in the  
21 ballot summary. And I definitely disagree with that.  
22 So Dr. Gilbert's sentence is written as if those two  
23 things are the same thing, but they are very  
24 different.

25 Q. So let's go back to paragraph 39C of

1 Dr. Gilbert's declaration. I apologize.

2 A. 39C.

3 Q. That would be Exhibit 6.

4 A. Yes.

5 Q. So that subparagraph reads: Ambiguous marks  
6 cannot occur on a BMD. The voter's intent is clear  
7 in the ballot summary and an auditor will not be  
8 asked to interpret voter intent.

9 Right?

10 A. That's what it reads.

11 Q. Okay. So the first part of that sentence,  
12 ambiguous marks cannot occur on a BMD, do you  
13 disagree with that?

14 A. I agree that ambiguous marks is generally  
15 not a problem with BMDs. Ambiguous marks can occur  
16 but are not necessarily significantly enough for me  
17 to disagree with the first seven words of Professor  
18 Gilbert's 39C.

19 Q. Okay. And ambiguous marks in the sense of,  
20 say, on a hand-marked paper ballot at a voter writing  
21 an X over the name or crossing out a line, those  
22 types of things don't happen on a BMD, right?

23 A. That's right.

24 Q. So what type of ambiguous marks are you  
25 referring to?

1           A.     Some BMD's may have printers that don't  
2     print very clearly.

3           Q.     So like if a printer is running out of ink,  
4     for example?

5           A.     Right; or just a printer is badly adjusted.

6           Q.     Low quality printer?

7           A.     Low quality printer.

8           Q.     Okay. And in last portion of that sentence,  
9     it says: An auditor will not be asked to interpret  
10    voter intent.

11                  Do you see that?

12           A.     Yes.

13           Q.     And do you disagree with that statement?

14           A.     No. I think that statement is -- that part  
15    of the statement is generally accurate.

16           Q.     So your quibble here is the voter's intent  
17    is clear in the ballot summary; is that right?

18           A.     I think it's more than a quibble. I think  
19    it goes to the heart of this case.

20           Q.     Okay. I'll rephrase it as your disagreement  
21    here. Would that be accurate?

22           A.     That's right.

23           Q.     Okay. And can you explain to me why that  
24    is?

25           A.     If the BMD is malfunctioning, especially if



1 it's malfunctioning because it's been hacked to  
2 cheat, it may well print on to the ballot summary a  
3 candidate selection that completely disagrees with  
4 the voter's intent as the voter expressed it in  
5 touching the touch screen. So in that case the  
6 voter's intent would be absolutely not clear in the  
7 ballot summary.

8 Q. Got it.

9 So the only time where you disagree with the  
10 voter's intent being clear is with respect to a  
11 malfunctioning BMD whether because of hacking or  
12 other reasons? Is that accurate?

13 A. That's right.

14 Q. Okay. So let's go back to Exhibit 3, and  
15 that would be your July -- the date of June 28, 2021.  
16 I apologize. I will mix those up. I refer to them  
17 as July because that's when they were served to us --

18 A. Got it.

19 Q. -- just so -- so if you'll scroll with me to  
20 paragraph 12.

21 A. Got it.

22 Q. You state there: I've not been asked to  
23 perform a forensic cyber security examination of any  
24 specific voting machine.

25 Do you see that?

1 A. Yes.

2 Q. And is that still accurate?

3 A. Yes.

4 Q. Have you performed any other type of  
5 examination of a specific voting machine for your  
6 report in this case?

7 A. In this case, no.

8 Q. Okay. Of course, you've looked at many  
9 different voting machines, many different kinds of  
10 examinations. Would that be right?

11 A. I have performed some examinations of  
12 specific voting machines myself, and I have read the  
13 scientific literature for detailed descriptions of  
14 other examinations of other voting machines, yes.

15 Q. Okay. And have you read the scientific --  
16 excuse me. I'm going to strike that. There's a fire  
17 truck passing. I apologize.

18 Have you read the scientific literature or  
19 any other reports as it relates to the Dominion  
20 voting machines utilized in Georgia?

21 A. I've read various things about the Dominion  
22 machines, but I have not read a cyber security  
23 examination report for those machines.

24 Q. What kind of things have you read about the  
25 machines?

1           A.    I've read the Dominion literature. I may  
2    have read the independent test lab report. I may  
3    have interviewed people who have used similar types  
4    of Dominion machines in other states.

5           Q.    When you say interviewed people, who did you  
6    interview?

7           A.    Most recently I talked to a voter in Camden  
8    County, New Jersey, who used a similar machine in  
9    2019.

10          Q.    Just a general voter you found?

11          A.    She had contacted me because she was  
12    interested in Camden County's selection process for  
13    voting machines.

14          Q.    Do you recall this person's name?

15          A.    Rena, R-E-N-A, and I can't recall her last  
16    name at the moment.

17          Q.    That's okay.

18                So in light of not performing any  
19    examination of the machines utilized in Georgia, you  
20    don't feel that prevents you from offering your  
21    opinions in here; is that right?

22          A.    That's right.

23          Q.    Okay. And sort of related to the not  
24    examining machines, have you examined any other  
25    election system adjacent items utilized in Georgia?

1 And by that I mean items like the voter registration  
2 database or the IT infrastructure of the Secretary of  
3 State's office?

4 A. No.

5 Q. And with respect to specific voting machine,  
6 would that include the poll pads used for voter  
7 check-in?

8 A. I have not examined those.

9 Q. Okay. So if you'll scroll with me to  
10 paragraph 20.

11 A. Yes.

12 Q. And you say there: It is a clear scientific  
13 consensus that any computer-based voting machine can  
14 be hacked.

15 Do you see that?

16 A. Yes.

17 Q. Do you understand any expert in this case to  
18 disagree with you on that statement?

19 A. No.

20 Q. So you go on in paragraph 21 to say: It is  
21 a clear scientific consensus that the only practical  
22 solution to this problem (that is secure enough for  
23 use in public elections) is to mark votes on  
24 voter-verified paper ballots that can be recounted or  
25 audited by hand.

1 A. That's right.

2 Q. Okay. So then in paragraph 22 you go on to  
3 say: There's clear evidence and a growing scientific  
4 consensus that ballots -- paper ballots marked by  
5 touch screen ballot marking devices are not voter  
6 verified in a strong enough sense to secure  
7 elections.

8 Do you see that?

9 A. Yes.

10 Q. You go on to say: And there's no known way  
11 of remedying the problem other than to abandon BMDs  
12 except for those voters who cannot mark a paper  
13 ballot with a pen.

14 Right?

15 A. Right.

16 Q. So in this paragraph you get more specific.

17 A. That's right.

18 Q. And when you say growing scientific  
19 consensus, what do you base that on?

20 A. I base that on many discussions that I've  
21 had with experts. I base it on the process conducted  
22 by the verified voting foundation which has many  
23 experts on its board of technical advisors and its  
24 board of directors who are independent of me and will  
25 not believe something just because I say so but will

1 come to their own scientific conclusions, who  
2 discussed this question mostly in the year 2019 and  
3 came to their formal recommendation that BMDs should  
4 not be used for voters who can mark a ballot with a  
5 pen.

6 I based it on, you know, my discussions with  
7 other independent experts who by the end of 2019 had  
8 come to this conclusion; and I find almost no  
9 experts -- so consensus does not mean unanimity. I  
10 know for example that Dr. Gilbert does not fully  
11 agree with me on this, that this really is a  
12 consensus and it's driven by scientific findings both  
13 about voter behavior of human beings who actually  
14 vote and of the inability of election procedures to  
15 correct the problem if there is some evidence of it.

16 Q. Okay. So I don't want to parse words too  
17 much here, but that's what us lawyers do. So the  
18 difference between paragraph 21 and paragraph 22, if  
19 you've got those there in front of you.

20 A. Yeah.

21 Q. You state in paragraph 21: It is a clear  
22 scientific consensus that the only practical solution  
23 to this problem is to mark votes on voter-verified  
24 paper ballots that are recounted or audited by hand.

25 And that's what we discussed earlier that

1 isn't specific as to one type of mark on the ballot  
2 or the other. Is that accurate?

3 A. I would say that paragraph 21 is an accurate  
4 description of the scientific consensus in 2018 and  
5 an accurate description of the scientific consensus  
6 in 2022; but paragraph 22 addresses an issue, the  
7 significance of which was not recognized generally by  
8 scientists in 2018 and was clearly recognized by  
9 2020.

10 Q. So at the time you wrote this declaration,  
11 which I think we saw earlier, was June 28, 2021,  
12 right?

13 A. Yes.

14 Q. Do you recall that?

15 A. Yes.

16 Q. Okay. In paragraph 22 there, you use some  
17 slightly different terminology. Rather than a clear  
18 scientific consensus, you say a growing scientific  
19 consensus. Is there a distinction there?

20 A. Yes. There's not a perfect way that one can  
21 measure exactly the scientific consensus among all  
22 the experts in a given field on any particular day,  
23 and the scientific consensus doesn't change all at  
24 once in one day.

25 Q. So, Dr. --

1           A.     When I wrote that paragraph 22, I did not  
2     want to make a stronger statement than I could  
3     absolutely warrant at that time. I will say, though,  
4     that it is the scientific consensus -- it's not an  
5     anonymous consensus, but it is the scientific  
6     consensus that elections conducted with most voters  
7     using BMDs are not securable, not fully auditable,  
8     and audits cannot reliably detect or correct the  
9     effects of hacking.

10           Q.     So, Dr. Appel, I'm going to note one more  
11     time an objection for a nonresponsive answer. I do  
12     appreciate you're trying to explain here, and you're  
13     welcome to explain after you answer the question.

14                     My question to you is, did you intend a  
15     specific distinction between paragraph 21 and  
16     paragraph 22, yes or no?

17           A.     Yes.

18                     MR. CROSS:   Objection; asked and answered.

19     BY MR. MILLER:

20           Q.     And that distinction you were intending  
21     there, is that what you were just describing to me?

22           A.     Yes.

23           Q.     Okay. But at the time you wrote this, am I  
24     incorrect in taking from this you did not believe  
25     there was a clear scientific consensus as to



1 represents the true scientific consensus to the  
2 best of our ability of the broader scientific  
3 community; and in June of 2018, the best of our  
4 ability to represent the true scientific  
5 consensus was as it was in 2018.

6 BY MR. MILLER:

7 Q. Okay. And so it changed, in your opinion,  
8 the true scientific consensus definitely between 2018  
9 and 2021. Do I have that right?

10 A. Yes.

11 Q. About when did that shift occur?

12 A. Mostly during 2019.

13 Q. So throughout 2018, in your opinion -- I'm  
14 not talking about the scientific consensus -- you  
15 still agree that this was consistent with -- with --  
16 strike that.

17 Throughout 2018, it is your opinion that the  
18 scientific consensus remains what was reflected in  
19 the NASEM report, right?

20 A. Right.

21 Q. It says, some time in 2019 on -- I'm trying  
22 to nail down where this shift occurred in your  
23 opinion.

24 A. Right. I would say the shift occurred  
25 mostly during 2019.

1 Q. Okay. So if we go back to Exhibit 3 of your  
2 July 2021 expert report.

3 A. Got it.

4 Q. If you'll turn to page 13 with me.

5 A. All right.

6 Q. And on page 40 there you draw a distinction  
7 between voter-verifiable paper ballots and  
8 voter-verified paper ballots. Do you see that?

9 A. Yes.

10 Q. Okay. Can you explain that distinction to  
11 me?

12 A. Yes. These are terms that had been used  
13 more or less interchangeably between, let's say, 2003  
14 and 2010, maybe even up to 2018. The  
15 voter-verifiable paper ballot is one that a voter  
16 could look at and read to see what candidates are  
17 indicated either by having their names printed or by  
18 having an oval blackened next to the name of a  
19 candidate as opposed to an unverifiable ballot such  
20 as one that's encoded in a QR code or not even  
21 printed on paper at all but hidden inside the memory  
22 of some computer.

23 So a voter-verifiable paper ballot is one  
24 that a voter could look at and read. A  
25 voter-verified paper ballot is one that a voter has

1 actually looked at and checked, that is to say  
2 verified, that it contains the candidate selections  
3 that the voter had indicated and intended.

4 Q. So would my understanding be correct that a  
5 voter-verifiable paper ballot can become a  
6 voter-verified paper ballot depending on the action  
7 of the voter?

8 A. That's right.

9 Q. Okay. And, in your opinion, would that  
10 apply to BMD ballots as used in Georgia?

11 A. The BMD ballots as used in Georgia can be  
12 voter-verifiable paper ballots depending on how  
13 election procedures and auditing procedures and  
14 recount procedures handle the difference between QR  
15 codes and the human readable portion of the ballot,  
16 but generally the plain text portion of a BMD ballot  
17 is a voter-verifiable paper ballot. It is not  
18 generally a voter-verified paper ballot.

19 Q. But just so that I am clear, it can become a  
20 voter-verified paper ballot if the voter looks at it  
21 and you mentioned election procedures, auditing, and  
22 recounts. We talked about that in detail but --

23 A. Right. Generally, yes, a BMD ballot as used  
24 in Georgia can become a voter-verified paper ballot  
25 if the voter reads it carefully with the exception of

1 the QR code printed on the ballot, which can never be  
2 a voter-verified paper ballot.

3 Q. So if you rule out a hack or a malfunction  
4 of the BMD with respect to the QR code, you would  
5 agree that can always become a voter-verified paper  
6 ballot depending on the action of the voter?

7 MR. CROSS: Objection to form. It misstates  
8 facts.

9 BY MR. MILLER:

10 Q. Do you understand the question I'm asking,  
11 Dr. Appel?

12 A. Yeah. The human readable portion of  
13 the BMD -- of the BMD ballot used Georgia that lists  
14 all the candidate selections can become a  
15 voter-verified paper ballot if the voter reads and  
16 studies it carefully and compares it to the voter's  
17 own memory of what choices they indicated.

18 Q. Okay. And have you done any study yourself  
19 on the accuracy rate of hand-marked paper ballots  
20 reflecting voter intent?

21 A. No. I read several other scientific studies  
22 and I have studied the data from the Minnesota 2008  
23 senate contest, which was a recount of 3 million  
24 hand-marked paper ballots, to see what the evidence  
25 indicated there about ambiguous marks on paper. So

1           So with respect to this sentence in  
2 paragraph 27, if a malicious actor were to install a  
3 fraudulent program that switches both the printed  
4 text and the QR code, would you -- would you agree  
5 with me that an individual voter would not be  
6 disfranchised if they verify their ballot?

7           MR. CROSS: Objection to form.

8 BY MR. MILLER:

9           Q. Do you understand my question, Dr. --  
10 Dr. Appel?

11          A. Yeah. So I would like to distinguish  
12 between human individual voters and exceptional  
13 individual voters.

14          Q. Dr. Appel, I'll ask you briefly if you could  
15 answer the question yes or no and then, of course,  
16 feel free to explain.

17          MR. CROSS: Carey, don't interrupt him.

18          Okay?

19          Go ahead, Doctor.

20          THE WITNESS: If an individual voter were to  
21 spend the 30 to a hundred or more seconds to  
22 inspect each contest on the ballot -- and the  
23 amount of times it takes will depend on how many  
24 contests are on the ballot -- to read carefully  
25 the name of the candidate selected and compare it

1 with who they indicated on the touch screen that  
2 they were voting for, then a person like that  
3 could defend themselves against their own ballot  
4 being hacked by a BMD. And unfortunately human  
5 voters can't or won't generally do that.

6 When a voter votes on a ballot-marking  
7 devices installed and supervised by the  
8 government, they are generally trusting that the  
9 ballot-marking device will indicate on the paper  
10 the selections they made on the touch screen.  
11 And measurements of real people show that they  
12 generally do not and cannot accurately notice  
13 errors. And I make a distinction between do not  
14 and cannot.

15 They do not and they don't understand the  
16 importance of checking the paper and as seen in  
17 practice, they generally don't check the paper;  
18 and they cannot in the sense that it is actually  
19 quite difficult to read a long, complicated  
20 ballot paper, especially when there's more than  
21 five or ten contests on the ballot, and actually  
22 notice a difference.

23 Humans are better at marking something than  
24 they are at proofreading something, especially in  
25 the kind of ballot formats printed by BMDs. All

1 of what I am saying has been measured in  
2 scientific studies.

3 BY MR. MILLER:

4 Q. Okay. So the first part of your answer  
5 there when you said a voter who was very astute, paid  
6 attention and read every single aspect could avoid  
7 this disenfranchisement; is that correct?

8 MR. CROSS: Objection to form.

9 THE WITNESS: Yes; up to the limits of even  
10 such a voter's ability to accurately proofread,  
11 which is less perfect than one might imagine.

12 BY MR. MILLER:

13 Q. Okay. Does that proofreading concept apply  
14 to hand-marked paper ballots?

15 A. Generally, the mark made by a pen on a  
16 hand-marked paper ballot is actually the mark that  
17 the voter indicated. Whereas, on a ballot-marking  
18 device, the voter indicates something on the touch  
19 screen by touching a specific place; and what's  
20 printed on the ballot card may vastly differ from  
21 that if the BMD is malfunctioning. There is no way  
22 on a hand-marked paper ballot to have a different  
23 mark on the paper than the one that the voter  
24 actually indicated.

25 Q. So you used the term "indicated" there, but

1 Q. Okay. All right. If you'll turn with me  
2 briefly to paragraph 85 of this report.

3 A. Exhibit 3?

4 Q. I'm sorry. Yes.

5 A. Got it.

6 Q. Here you're talking about accessible voting  
7 machines for disabled voters, right?

8 A. Yes.

9 Q. Okay. So in paragraph 85 here, you use the  
10 phrase "I know of no perfect design." Do you see  
11 that?

12 A. Yes.

13 Q. And then above that in paragraph 84, you  
14 say, this is not a perfect solution, right?

15 A. Right.

16 Q. I didn't understand your opinion as to use  
17 of hand-marked paper ballots to be one that such a  
18 system is perfect for the general populace. Am I  
19 wrong on that?

20 A. Nothing is perfect; but with hand-marked  
21 paper ballots, it's possible to conduct a secure and  
22 accurate election even in the presence of  
23 computerized voting machines that may be hacked and  
24 may be trying to cheat. And with the use of BMDs, it  
25 is not possible to conduct secure and accurate



1 elections in the presence of computerized voting  
2 systems that have been hacked. So hand-marked paper  
3 ballots successfully resist the efforts of hacked  
4 voting machines to corrupt elections and BMD-marked  
5 ballots cannot.

6 Q. Okay. I guess my question here is more of  
7 the use of the term "perfect design" here.

8 A. Right.

9 So I guess what I'm referring to in  
10 paragraphs 84 and 85 is that they may contemplate the  
11 use of BMDs for voters with disabilities that lead  
12 them unable to mark a paper ballot by hand even  
13 though that solution will not fully protect their  
14 vote in the case that computerized voting systems may  
15 be hacked.

16 In that sense, voters with disabilities who  
17 would use BMDs would have somewhat less protection of  
18 their vote than voters who were able to mark a paper  
19 ballot by hand. Such voters may still have some  
20 protection, and they can get it by the means that I  
21 described in paragraph 84, and they can get it in  
22 other ways. So that's what I'm talking about in  
23 paragraphs 84 and 85.

24 Q. Okay. All right. Dr. Appel, if it's okay  
25 with you, I'm going to suggest we take a short break

1 this, right?

2 A. Yes.

3 Q. Okay. Are you aware of fraudulent software  
4 like that that self-propagates to multiple BMDs?

5 A. Yes.

6 Q. And where is that?

7 A. The concept of fraudulent software that  
8 propagates on removable media from one computer to  
9 another, not specifically in the context of  
10 elections, was first explained to me in approximately  
11 1979. And the first demonstration of this on actual  
12 voting machines was done by a scientific study at  
13 Princeton University in -- published in 2006 where it  
14 was done on the exact model of voting machine that  
15 was in use in Georgia between about that time and  
16 2018.

17 Q. So I think my question was a little more  
18 specific to that as to BMDs. Are you aware of such  
19 software existing?

20 A. Am I aware that someone has created any such  
21 software specifically for a BMD, no.

22 Q. Okay. And in that Princeton study you were  
23 referring to, how did that fraudulent software  
24 self-propagate?

25 A. It propagated on the removable media that

1 election administrators used to download the ballot  
2 definition file from the county election  
3 administration computer to the voting machine.

4 Q. And --

5 A. And then they used that same removable media  
6 to upload the vote results from the voting machine to  
7 the county election administration computer; and the  
8 hack, the vote stealing virus, could piggyback on  
9 that removal media in both directions to go from one  
10 voting machine to a county election administration  
11 computer and then from that computer to many other  
12 voting machines and so on.

13 Q. And this fraudulent software that you refer  
14 to on the DREs, was it adaptable to multiple ballot  
15 styles?

16 A. It's certainly straightforward to write  
17 software that's adaptable to multiple ballot styles.  
18 I'm not sure whether that particular thing was  
19 demonstrated in the 2006 scientific paper.

20 Q. Okay. So conceptually you believe that it  
21 could be done. Is that accurate?

22 A. Yes.

23 Q. But you've never seen such adaptable  
24 self-propagating software on the DREs; is that right?

25 A. I've seen adaptable vote stealing software

1 that automatically adapts itself to different ballot  
2 styles. This is pretty easy to write given that a  
3 typical ballot style will identify the political  
4 party of each candidate. So the vote stealing  
5 software doesn't have to work very hard to figure out  
6 which is the Republican and which is the Democrat.  
7 And I have seen vote -- you know, self-propagating  
8 software. I haven't specifically seen the  
9 combination of self-propagating and adaptable  
10 software, but that would entirely straightforward to  
11 combine.

12 Q. Okay. I don't mean to pump your ego here,  
13 but you're a preeminent expert in this field, right?

14 A. Yes.

15 Q. But you haven't seen that combination?

16 A. No.

17 Q. Okay. Let's -- I'm going to share with you  
18 another exhibit here.

19 (Exhibit 9 was marked for  
20 identification, attached at the end of  
21 the original transcript.)

22 BY MR. MILLER:

23 Q. Just let me know when it shows up on your  
24 end.

25 A. Got it.

1 Q. On 30,000 BMDs, right?

2 A. Okay.

3 Q. And let's assume that implanting the same  
4 malware or similar malware -- strike that.

5 Let's assume that implanting the vote  
6 flipping fraudulent software takes about the same  
7 time as your demonstration in the New Jersey case,  
8 seven minutes. Okay?

9 A. I don't know why we would assume that.

10 Q. Do you have any reason to think it would be  
11 shorter or longer?

12 A. Yeah. It would be much different, actually.  
13 If one wanted to install fraudulent software on any  
14 machines statewide in the kind of modern system used  
15 in Georgia now or in the kind of DRE that Georgia  
16 used between 2003 and 2018, one would not have to do  
17 it one machine at a time with a screwdriver. One  
18 would generally do it with automatic propagation  
19 particularly from one machine to another, although  
20 that's possible but more likely from one central  
21 place to all the machines. The central place could  
22 be state election administration computers, county  
23 elections administration computers or a hacker who  
24 manages to hack into Dominion election systems  
25 itself. So I would not expect that the most

1 efficient method a hacker could use is to do it one  
2 machine at a time by a screwdriver.

3 Q. We just discussed that you're not aware of  
4 both self-propagating and adaptable malware, right?

5 A. I'm aware of how straightforward it is in  
6 principal to build each of those and combine them  
7 together. I am not aware of a hacker who has done  
8 that to an actual BMD.

9 Q. Whether in a lab or in an actual election,  
10 right?

11 A. Right.

12 Q. So if you're not aware of it, let's talk  
13 about what we know you are aware of, which is  
14 individually adaptable but not self-propagating,  
15 right?

16 A. Yeah.

17 Q. Okay. So that would require access to  
18 individual BMDs; would it not?

19 A. If it's not self-propagating.

20 Q. Okay.

21 A. Well, there's self-propagating and -- yeah.  
22 All right. If you want to -- if you want to talk  
23 about malware that does not propagate by means of  
24 network server removable media, that would require  
25 access to individual BMDs.

1 Q. I'm trying to use the same terminology  
2 you --

3 A. Yeah. I'm not aware of a specific piece of  
4 malware that is both self-propagating and adaptable,  
5 but there is no scientific difficulty in combining  
6 those two concepts into the same piece of malware.

7 Q. Okay. But you've never done it?

8 A. I've never done it.

9 Q. And you're not aware that anybody has ever  
10 done it, right?

11 A. Right.

12 Q. Okay. So accepting that, let's talk about  
13 what we are aware of, which is adaptable but not  
14 self-propagating, right?

15 A. We can talk about adaptable but not  
16 self-propagating malware.

17 Q. So do you have -- going back to the  
18 seven-minute timeframe, do you have any reason to  
19 believe implanting that adaptable but not  
20 self-propagating malware into a BMD would take any  
21 shorter or longer time than what it took you to  
22 implant it on this --

23 A. I would expect it would take a shorter time.  
24 The seven minutes it took me to install the malware  
25 in a Sequoia AVC Advantage BMD required, you know,

1 picking the lock on the door of the voting machine,  
2 unscrewing ten screws, prying out one computer chip,  
3 installing another computer chip in its place,  
4 replacing a certain cover that was held down by those  
5 ten screws, screwing back in the ten screws, closing  
6 the door and picking the lock again to get it to  
7 lock.

8 And on a more modern piece of equipment, it  
9 might well be possible to install malware by just  
10 sticking a USB cartridge into a slot for five  
11 seconds.

12 Q. Okay. So --

13 A. It really depends on the voting machine.

14 Q. Okay. So five seconds -- if you wanted to  
15 infect BMDs statewide, you would need access to those  
16 machines, right?

17 MR. CROSS: Objection to form.

18 THE WITNESS: In this hypothetical where one  
19 is not doing it by the more efficient method of  
20 automatically propagating it.

21 BY MR. MILLER:

22 Q. Correct.

23 But if you use your seven-minute estimate,  
24 my back-of-the-napkin math is that's 210,000 minutes  
25 of total time just implanting the malware, right?



1 MR. CROSS: Objection to form.

2 THE WITNESS: Yeah. If Georgia were using  
3 Sequoia AVC Advantage DREs and someone wanted to  
4 install the same kind of malware I installed in  
5 2008 into one of those at seven minutes per, that  
6 would be 210,000 minutes.

7 BY MR. MILLER:

8 Q. And you are -- strike that.

9 Are you aware of who the responsibility for  
10 storing voting machines falls on in Georgia?

11 A. Not specifically.

12 Q. Would you have any reason to doubt me if I  
13 represent to you that each county is responsible for  
14 storing their voting equipment consistent with state  
15 law and regulations around physical security?

16 MR. CROSS: Objection to form. It misstates  
17 facts.

18 THE WITNESS: Certainly in a lot of states  
19 each county is responsible for -- each county's  
20 election officials are responsible for the  
21 storage of their own county's voting machines.  
22 So I could easily believe that Georgia organizes  
23 itself that way.

24 BY MR. MILLER:

25 Q. Are you aware there are 159 counties in

1 Georgia?

2 A. I'm aware there's something like that.

3 Q. An unreasonably large number.

4 And so, of course, to implant any malware  
5 you would have to have knowledge of where those BMDs  
6 are stored and arranged in our hypothetical scenario,  
7 right?

8 MR. CROSS: Objection to form.

9 THE WITNESS: In this hypothetical scenario  
10 where the hacker is choosing to use this  
11 inefficient method of attacking each machine  
12 retail, then -- instead of centrally wholesale,  
13 then they need access to as many machines as they  
14 want to hack.

15 Number one, it's not necessary for them to  
16 hack all 30,000 machines in order to get a whole  
17 lot of votes to be switched. Number two, it's  
18 not necessary to hack them while they're in the  
19 county's election warehouse. I have been in  
20 election warehouses in a couple of different  
21 states, and I can say that the security of  
22 election warehouses is not always as good as one  
23 might want.

24 And then the other point is that there may  
25 be places to access these voting machines when

1       they're not in election warehouses such as when  
2       they're being transported to the polling places,  
3       when they're in the polling places before or  
4       after an election, or whether -- where they're  
5       being transported from the polling places.

6               And you might think that when voting  
7       machines are being transported from the polling  
8       places after an election it's too late to hack  
9       them to make them misbehave in that election, but  
10       it's not too late to install adaptable vote  
11       stealing software that will misbehave in many  
12       future elections.

13               So there are a variety of places that an  
14       attacker might have access to voting machines to  
15       be able to install fraudulent malware that may  
16       misbehave in future elections for a decade or  
17       more.

18       BY MR. MILLER:

19               Q.    Have you ever been to an election warehouse  
20       in Georgia?

21               A.    No.

22               Q.    Have you ever been to a polling place in  
23       Georgia?

24               A.    No.

25               Q.    Do you have any knowledge of the security

1 Q. And would you agree with me that it's a  
2 continuum of sorts on the acceptability of the use;  
3 in other words, DREs are way out on the bad side in  
4 your opinion and paper ballots are way out on the  
5 good side and in between you have the DRE with VD  
6 pad, all-in-one BMDs, and BMDs like those used in  
7 Georgia?

8 MR. CROSS: Objection to form.

9 THE WITNESS: Are you talking about my  
10 opinion or are you talking about the current  
11 scientific consensus? Are you talking about the  
12 scientific consensus.

13 BY MR. MILLER:

14 Q. That's a fair point. That's a fair point.  
15 I'm talking about your opinion here.

16 Would you agree with me that there are  
17 levels of acceptability, for lack of a better term,  
18 on each form of voting system?

19 A. I would say that DREs are unacceptable.

20 Q. Right.

21 A. DREs with a VD pad are unacceptable in light  
22 of current scientific understanding. All-in-one BMDs  
23 that display something behind glass or that have the  
24 ability to both mark a ballot and deposit it in a  
25 ballot box are unacceptable. Those are not at issue

1 in this case. And BMDs are acceptable for use only  
2 for those voters who cannot mark a paper ballot by  
3 hand.

4 Q. Okay. And then the next step would be  
5 optical scan -- hand-marked paper ballots with  
6 optical scanners are acceptable, period, your  
7 preferred system in your opinion for security  
8 reasons?

9 A. Right.

10 Q. Okay. So if you scroll with me here to page  
11 3 and it's your footnote 2.

12 A. All right. I read footnote 2.

13 Q. You talk about the understandable preference  
14 of mainstreaming disabled voters, right?

15 A. Right.

16 Q. And you say that's a legitimate desire, but  
17 on balance you think the competing legitimate desire  
18 for trustworthy election outcomes wins out. Is that  
19 accurate?

20 A. Right.

21 Q. Is this statement assuming the presence of  
22 malware that you have actual knowledge of versus the  
23 presence of malware that in theory could be created?

24 A. The statement is in view of the  
25 susceptibility of computerized voting equipment to be

1 hacked by malware.

2 Q. To be hacked by malware that you have actual  
3 knowledge of or that conceptually you believe could  
4 be developed?

5 A. The ability of computers to be reprogrammed  
6 with new software has been an essential feature of  
7 the concept of the computer since 1950 when the  
8 stored program computer was invented. So it is an  
9 inherent aspect of a computer that it can be  
10 reprogrammed, that -- and so any voting machine based  
11 on a computer can be hacked, can be reprogrammed.

12 This has been demonstrated repeatedly on one  
13 kind of voting machine after another after another  
14 after another, but it's such an inherent part of the  
15 nature of a computer that you can download new  
16 software into it that in some sense it didn't even  
17 need to be demonstrated on one kind of voting machine  
18 after another after another. And so it's an inherent  
19 fact of computer science that the next voting  
20 machine, if it's run by software in a computer, will  
21 be hackable.

22 Q. I think you may be misunderstanding my  
23 question.

24 With your statement that this is made in  
25 light of your opinion on the hackability of a

1 malware that could adapt and self-propagate right in  
2 theory?

3 A. Right. Right.

4 Q. And I should ask a clarifying question. I  
5 noticed in your report you for the most part stick to  
6 the term "fraudulent software" as opposed to malware.  
7 Is there a distinction there or is that a term of  
8 art?

9 A. I guess by fraudulent software I mean  
10 software that pretends to be what it's not. Some  
11 malware does that. Some malware is more explicit and  
12 doesn't even try and pretend.

13 Q. Okay. So are you aware of -- strike that.

14 Based on your opinion, knowledge, and  
15 experience do you believe conceptually malware or  
16 fraudulent software could be implanted on to a DRE  
17 and snake its way into the Dominion BMDs?

18 A. Yes. I think that would be possible,  
19 although it doesn't seem the most likely way that a  
20 hacker might want to install malware on the Dominion  
21 BMDs.

22 Q. And, of course, that would have to have been  
23 installed prior to the last use of the DRE -- DREs  
24 themselves, right?

25 MR. CROSS: Objection to form.

1 THE WITNESS: If what you're trying to say  
2 is should we be worried about the particular  
3 pathway of someone installing malware in a  
4 Diebold BMD or in GEMS and then that propagating  
5 to the Dominion systems, I would say that is not  
6 a likely way for a malware to propagate to the  
7 Dominion systems. There are other ways that  
8 hackers would be more likely to use than that to  
9 propagate malware on to the Dominion systems.

10 And part of the reason for that is that if  
11 the Diebold system has not recently been in use,  
12 then the malware would have had to have been  
13 installed on it at the time it was, you know,  
14 turned on. So that's not the pathway I would  
15 most worry about.

16 BY MR. MILLER:

17 Q. I do want to briefly clarify one point. I  
18 think you said Diebold BMD, but you meant Diebold  
19 DRE, right?

20 A. That is right.

21 Q. Okay. And for that malware or fraudulent  
22 software to work to flip a vote in the theoretical  
23 ways we've described, the person installing it on the  
24 DRE would have to have some knowledge as to the  
25 system that was follow -- following it, right?



1 MR. CROSS: Objection to form. It calls for  
2 speculation.

3 THE WITNESS: You know, I could describe  
4 another method by which malware in the GEMS  
5 system would make it easier for a hacker to flip  
6 votes on a Dominion BMD.

7 BY MR. MILLER:

8 Q. That's not the question I'm asking.

9 A. Well, it very closely related to the  
10 question you asked. You asked is it possible that  
11 malware on the Diebold system could flip votes on the  
12 Dominion BMD; and there's an assumption built into  
13 that question about how malware actually works, so I  
14 want to address that assumption.

15 One very important way that malware works is  
16 to open up back doors in computer systems that  
17 hackers can later use to exploit, and the way they  
18 might exploit it is by delivering a payload that  
19 actually does the malicious function such as stealing  
20 money or switching votes.

21 I would think it unlikely that somebody  
22 would have designed such a payload in 2018 for the  
23 Dominion BMDs that got delivered in 2019. It is  
24 certainly possible that malware installed in  
25 computers used to manage Georgia's elections could

1 have opened up back doors that might still remain in  
2 Georgia's current computers that manage Georgia's  
3 elections; but as to the question with the assumption  
4 that you built into it that this would be about the  
5 payload that switches votes, I would expect that that  
6 payload would not have been designed and installed  
7 into the Diebold machines and transfer itself to the  
8 Dominion machines.

9 Q. Okay. And so when I am talking about an  
10 election management system, do you understand that  
11 I'm referring to software that runs on a computer and  
12 not the computer itself?

13 A. All right. If you want to refer to it that  
14 way.

15 Q. And does it make any difference -- let me  
16 ask it this way. Is your statement there assuming  
17 that it's the same computer that the EMS software is  
18 running on or does it matter?

19 A. In this very hypothetical scenario we're  
20 talking about where an attacker who hypothetically  
21 managed to compromise Georgia's election systems in  
22 2018 or prior, they would still be able to leverage  
23 to still make it easier to compromise Georgia's  
24 election systems in 2019 and subsequent. The reuse  
25 of the same computers could be relevant if Georgia is

1 concerned if you were to learn that election workers  
2 were using USB devices with the new BMD system that  
3 they previously had used with the old DRE system?

4 A. Yes, I would be concerned.

5 Q. Would that, in your opinion, be consistent  
6 with sound election security practices, meaning to  
7 use those same USB devices?

8 A. Right. In light of the insecurity of USB  
9 systems in general it's a general security  
10 recommendation, not just for elections specifically  
11 but in any application where you actually care about  
12 security, is not to reuse USB devices that have been  
13 out of your physical possession in places you don't  
14 necessarily trust. And so the idea of using fresh  
15 USB devices in every election or certainly using  
16 fresh USB thumb drives and you switch to a new set of  
17 equipment that would be a prudent security  
18 recommendation in general. I haven't studied it  
19 specifically on how it would apply to the machines in  
20 this case.

21 Q. As an elections security expert, would you  
22 be concerned if poll workers in Georgia were  
23 connecting USB drives to voting equipment that had  
24 also been connected to internet connected device like  
25 a server or a computer?

1           A.     Yes, absolutely. The kind of  
2     self-propagating malware that was identified and  
3     demonstrated as early as 2006, you know, in a  
4     scientific paper about voting equipment can propagate  
5     malware from computers in the sense of things that  
6     look like computers and have keyboards and screens to  
7     voting machines. So if you have computers that are  
8     routinely connected to the internet where they are  
9     vulnerable to attack from anywhere on the internet  
10    and then those computers may be corrupted, they can  
11    be corrupted in such a way as to distribute malware  
12    through USB devices to all the voting machines in the  
13    normal process of installing ballot definitions for  
14    each election. And this attack factor, this kind of  
15    vulnerability, has been well understood for about  
16    15 years now.

17           Q.    As an election security expert, would you be  
18    concerned if election workers in Georgia, the  
19    passwords that they use to access and operate voting  
20    equipment, if those passwords were transmitted via  
21    FTP?

22           A.    Yes, I would be concerned. FTP is an  
23    obsolete of method of transferring information over  
24    the internet, and the specific reason its obsolete  
25    for at least ten years now is because it is insecure.

1 It's not protected by encryption in any -- in any  
2 way. So any computer systems that you know want to  
3 transmit information like that will use other  
4 protocols now, and indeed even most modern browsers  
5 for compute -- you know, for consumer use have FTP  
6 disabled because it's not even safe enough for  
7 ordinary consumers to use.

8 Q. Related to that, Dr. Appel, as an elections  
9 security expert, would you be concerned if the  
10 passwords that election workers in Georgia use to  
11 access or operate voting equipment were stored on  
12 servers that are connected to the internet?

13 A. That would definitely be a concern. A  
14 servers connected to the internet are vulnerable to  
15 possible infiltration by hackers who can read and  
16 modify any data that's stored there. So that would  
17 be a way that hackers could potentially get access to  
18 those passwords.

19 Q. Do you know whether the current Dominion  
20 voting equipment that's used in Georgia can scan and  
21 tabulate hand-marked paper ballots?

22 A. I believe that it can.

23 Q. And could ballots that voters can mark by  
24 hand -- is there equipment available today for those  
25 to be printed at the precinct on demand?

1           A.    Yes.  So what you're talking about is called  
2   a ballot on-demand printer, and I've had  
3   conversations with Howard Kramer, the vice president  
4   of Dominion, about every -- about two or three times  
5   a year for the last two or three years about this  
6   line of Dominion election equipment.  Most of these  
7   conversations are not specifically motivated by my --  
8   by this Georgia case but just generally for the  
9   possible adoption of Dominion equipment in other  
10  states.

11                   And so he has very clearly clarified to me  
12  that these same scanners are compatible with  
13  hand-marked optical scanned paper ballots and that  
14  these same scanners are compatible with ballot  
15  on-demand printers.  These are basically ordinary  
16  desktop laser printers that would sit next to e-poll  
17  book where voters check in and it could print an  
18  unmarked optical scan paper ballot with ovals for the  
19  voter to fill in.  That these Dominion systems that  
20  Georgia already uses are adaptable to be used in this  
21  way at a fairly low additional cost, which is to say  
22  the ballot on-demand printers are not expensive.

23           Q.    And just finally here, Dr. Appel, can you  
24  pull up Exhibit 12 again?  Do you have that in front  
25  of you?

1 infrastructure?

2 A. Absolutely, yes.

3 Q. And based on your experience and expertise  
4 as an elections security expert, would you expect  
5 officials who are responsible for elections in the  
6 state of Georgia to take reasonable measures to  
7 address any security weakness Dr. Halderman  
8 identified in his analysis of the equipment?

9 A. Yes.

10 So although we know that computerized voting  
11 machines are vulnerable to hacks in general, we would  
12 certainly want to minimize as best we can the ability  
13 of hackers to get into those machines and perform  
14 hacks.

15 So when makers of election equipment take  
16 steps to improve the security of the equipment they  
17 sell, that's a good thing. When election  
18 administrators who deploy this equipment take steps  
19 to improve the security of their deployment, that's a  
20 good thing. When election administrators put  
21 pressure on the vendors who sell them equipment to  
22 improve the security of the equipment they sell,  
23 that's a good thing.

24 We should do all of these things even though  
25 we recognize that we can never fully defend against

1 hacks and so that we should run elections in a way  
2 that we can still trust in their accuracy even though  
3 the equipment may have been hacked.

4 Or to put it another way, when, for example,  
5 hand-marked paper ballots are used risk-limiting  
6 audits can detect and recount -- can correct  
7 elections that are inaccurate because of hacks or  
8 other failures; but we should improve the security of  
9 the computers and the computerized voting machines so  
10 that that's less likely to happen. It's less likely  
11 that flawed elections occur to be detected and  
12 recounts would be necessary to correct them.

13 Q. Dr. Appel, as a -- I think as Mr. Miller  
14 referred to you earlier, as a preeminent election  
15 security expert, is providing voters -- election  
16 officials themselves providing voters incomplete or  
17 inaccurate information about known security  
18 vulnerabilities in the election system -- is that a  
19 sound way to generate voter confidence in that  
20 election system?

21 MR. MILLER: Objection; relevance, lack of  
22 foundation.

23 Dr. Appel, you're permitted to answer over  
24 the objection.

25 THE WITNESS: Yeah. Let's -- I can -- I can



1 to specifically compare the QR code to the human  
2 readable text on the ballot as long as the entire  
3 risk-limiting audit or recount is done based only on  
4 the human readable portion of the ballot.

5 Q. Are you assuming that the official election  
6 count -- the official election results will then be  
7 based on the tabulation of the recount rather than  
8 the original tabulation from the machines?

9 A. If you recount what's written on the human  
10 readable portion of the ballots, which I'm not sure  
11 is always how recounts work in Georgia, and if the  
12 voters carefully reviewed the human readable portion  
13 of the ballots, which we know that most of them do  
14 not, then you could achieve a recount of the  
15 voter-verified intent.

16 If you leave out either of those portions  
17 and if the BMDs are hacked, then you cannot achieve a  
18 recount of the voter's intent. If you leave out  
19 examining the human readable portion of the ballot,  
20 then you're vulnerable to the attack by which the QR  
21 code is fraudulent but the human readable portion is  
22 accurate.

23 And if you leave out the voter spending a  
24 whole minute, you know, carefully reviewing every  
25 line of the ballot, then you're vulnerable to the

1 attack where both the QR code and the human readable  
2 portion are vulnerable.

3 Q. Lastly, Dr. Appel, if you look back at  
4 Exhibit 12, the fourth paragraph that Mr. Miller  
5 asked you about, the two sentence reads: Technical,  
6 physical, and procedural safeguards complicate the  
7 task of maliciously exploiting election systems as  
8 does monitoring of likely adversaries by law  
9 enforcement and the intelligence community.

10 Do you see that?

11 A. Yes.

12 Q. Why was the word "complicate" use instead of  
13 prevent in that sentence?

14 A. The unfortunate fact about computer security  
15 in this part of the 21st Century is we cannot prevent  
16 all attacks from being successful. Even the most  
17 sophisticated companies that produce software, that  
18 run data centers, that run commerce both brick and  
19 mortar and e-commerce and the U.S. government itself  
20 have been subject to malicious attacks and have  
21 successfully infiltrated their system and stolen and  
22 altered information.

23 So the modern state of cyber security is  
24 that defenses can help. They can complicate the life  
25 of the attacker. They can shut off the attack paths

1 that we know about, but they cannot shut off all the  
2 attack paths that we don't yet know about. So  
3 complicate the task is the best bet we know how to do  
4 in cyber security in general and election systems as  
5 an example of cyber security.

6 Q. Thank you, Dr. Appel.

7 FURTHER EXAMINATION

8 BY MR. MILLER:

9 Q. Dr. Appel, I've got just a couple of quick  
10 follow-up questions, and I'll be brief.

11 Do you recall Mr. Cross asking you about  
12 ballot on-demand printers?

13 A. Yes.

14 Q. Okay. And are you offering an opinion in  
15 this case regarding the feasibility of the  
16 Plaintiffs' requested relief?

17 A. To the extent that the relief involves the  
18 use of the same Dominion equipment that Georgia  
19 already has deployed but with ballot on-demand  
20 printers so that the voter is generally handed a  
21 paper ballot to fill out and only those voters who  
22 can't mark a paper ballot with a pen use the  
23 ballot-marking device, I am offering an opinion that  
24 that would be feasible, practical, and cost  
25 effective.

1 Q. So by feasible, practical, and cost  
2 effective first --

3 A. Feasible means available from the vendors.  
4 It does not require new scientific research to figure  
5 out.

6 Q. Right.

7 A. Meaning other states use this kind of ballot  
8 on-demand method and it works and cost effective in  
9 that, you know, the cost of ballot on-demand printers  
10 is actually significantly less than the cost of  
11 voting machines such as optical scanners and BMDs.  
12 So that the additional cost to add ballot on-demand  
13 printers to the Georgia system would not be nearly so  
14 great as the cost that Georgia has already invested  
15 in these systems already.

16 Q. Have you ever administered an election?

17 A. No.

18 Q. Have you ever worked as a poll worker?

19 A. No.

20 Q. Have you ever trained the local election  
21 officials on how to run a polling place?

22 A. No. I read the training materials.

23 Q. So is your statement that you are offering  
24 feasibility to the extent, do you mean by that you're  
25 offering an opinion on feasibility that the various

1 vulnerability that the good guys haven't discovered  
2 yet but maybe the bad guys have already.

3 Q. Correct.

4 Whack a mole, right?

5 A. Right.

6 MR. MILLER: That's all I have.

7 FURTHER EXAMINATION

8 BY MR. CROSS:

9 Q. One follow-up questions, Dr. Appel on the  
10 last point.

11 Is it sound cyber security practice to  
12 ignore known vulnerabilities simply because there may  
13 be other unknown vulnerabilities in an election  
14 system?

15 A. No.

16 MR. CROSS: No further questions.

17 THE VIDEOGRAPHER: This concludes the  
18 deposition. The time is 11:58 a.m., and we're  
19 now off the video record.

20 THE COURT REPORTER: Do y'all want to order  
21 the transcript?

22 MR. CROSS: Yes.

23 MR. MILLER: I think we have a standing  
24 order on this. We'll take a rough when it's  
25 available.

## 1 CERTIFICATE

2 STATE OF GEORGIA:

3 COUNTY OF GWINNETT:

4 I hereby certify that the foregoing  
5 transcript was taken down, as stated in the caption,  
6 and the colloquies, questions and answers were  
7 reduced to typewriting under my direction; that the  
8 transcript is a true and correct record of the  
9 evidence given upon said proceeding.


10 I further certify that I am not a  
11 relative or employee or attorney of any party, nor am  
12 I financially interested in the outcome of this  
13 action.

14 I have no relationship of interest in  
15 this matter which would disqualify me from  
16 maintaining my obligation of impartiality in  
17 compliance with the Code of Professional Ethics.

18 I have no direct contract with any  
19 party in this action and my compensation is based  
20 solely on the terms of my subcontractor agreement.

21 Nothing in the arrangements made for  
22 this proceeding impacts my absolute commitment to  
23 serve all parties as an impartial officer of the  
24 court.

25 This the 13th day of February, 2022.



---

LAURA R. SINGLE, CCR-B-1343